IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

IN RE: BPS DIRECT, LLC and CABELA'S, LLC, WIRETAPPING	**MDL NO. 3074** **2:23-md-03074-MAK**

PLAINTIFFS' OPPOSITION TO DEFENDANTS' MOTION TO DISMISS

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Rules

Other Authorities

INTRODUCTION

Plaintiffs Brian Calvert, Heather Cornell, Timothy Durham, Marilyn Hernandez, Greg Moore, Peter Montecalvo, Arlie Tucker, and Brittany Vonbergen (collectively "Plaintiffs") brought this class action against Defendants BPS Direct, LLC, d/b/a Bass Pro Shops ("BPS") and Cabela's LLC ("Cabela's") (collectively, "Defendants"), for facilitating the wiretapping of their electronic communications in violation of Plaintiffs' privacy rights and the rights of nationwide and state class members.[1] Defendants moved to dismiss the case for lack of subject matter jurisdiction and for failure to state a claim. ECF 54 (Motion); ECF 54-1 (Memorandum; hereinafter "MTD"). Defendants' motion should be denied in its entirety.

FACTUAL BACKGROUND

The fundamental factual premise of this case is undisputed: BPS and Cabela's embed snippets of JavaScript computer code ("Session Replay Code" or "SRC") on their websites provided by third-party vendors ("Session Replay Providers" or "SRPs"), which then deploys on each website visitor's internet browser for the purpose of intercepting and recording the website visitor's electronic communications with Defendants' websites. ¶¶ 3, 9, 64-87; *see also* ECF 47 at 3-6 (stipulated facts). The Session Replay Code procured and employed by Defendants tracked Plaintiffs' and Class Members' "mouse clicks and movements, keystrokes, search terms, substantive information inputted by Plaintiff[s], pages and content viewed by Plaintiff[s], scroll movement, and copy and paste actions." ¶ 99; *see also* ¶¶ 90-91 (SRC "provide[s] detailed information about user sessions, interactions, and engagement, with the capacity to break down

[1] Plaintiffs filed their Consolidated Class Action Complaint on August 14, 2023. ECF 53. References to the operative complaint are referenced by paragraph number throughout. All emphasis is added unless otherwise indicated.

users by device type, location, and other dimensions" and vendors "collected and continue to collect Plaintiffs' and Class Members' highly personal information and substantive communications that can be tied directly to a website user's identity as it monitors, records, and collects a website user's every move"). Plaintiffs allege this conduct constitutes a wiretap in violation of federal and state statutes, and that it invaded Plaintiffs' and Class Members' privacy and violated federal, state, and common law requirements.

Despite Defendants' characterization of their behavior as "common" and "routine," Plaintiffs plausibly allege that Defendants' conduct is highly intrusive, done without Plaintiffs' consent or ability to opt out, and intercepts troves of content, including personally identifiable and sensitive information by recording individual browsing sessions that are then transmitted to third parties for use in marketing, tracking, and other purposes. ¶¶ 7, 68-96. The privacy invasions are extensive. SRC as implemented and procured by Defendants prevents users from remaining anonymous, allows third parties to capture information from Plaintiffs *even if they do not submit that information to Defendants*, exposes website visitors to identity theft, online scams, and data breaches, gives unvetted third parties access to private information captured by websites, and operates in violation of industry best practices. ¶¶ 72-87. These purposes far exceed the "website functionality" purposes Defendants espouse and violate consumers' reasonable expectations. ¶ 72.

ARGUMENT

I. Plaintiffs Adequately Plead Article III Standing.

A. Plaintiffs Have Standing to Bring These Claims.

Defendants challenge whether Plaintiffs have suffered an injury in fact, despite binding, on-point Third Circuit case law. To make their argument, Defendants would have this Court focus its attention on the sensitivity of the content. This is incorrect pursuant to Third Circuit precedent.

The harm stems from the conduct of the intrusive and surreptitious wiretapping itself, regardless of the sensitivity of the content captured. "To allege an injury-in-fact, a plaintiff must claim the invasion of a concrete and particularized legally protected interest resulting in harm that is actual or imminent, not conjectural or hypothetical." *In re Nickelodeon Cons. Priv. Litig.*, 827 F.3d 262, 271 (3d Cir. 2016) (citations omitted). A harm is particularized if it affects the plaintiff in a personal and individual way. *Id.* It is concrete if it is *de facto*; it must actually exist rather than being only abstract. *Id.* In analyzing standing, a court must be careful to separate the standing inquiry from *any assessment of the merits of plaintiff's claims*. *Weichsel v. JP Morgan Chase Bank*, 65 F.4th 105, 111 (3d Cir. 2023) (citing *Cottrell v. Alcon Lab'ys*, 874 F.3d 154, 162 (3d Cir. 2017)).

When evaluating whether an alleged harm qualifies as an injury-in-fact, the Court should examine whether the codified injury "has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American Courts." *Spokeo, Inc. v. Robins*, 578 U.S. 330, 341 (2016); *see also TransUnion v. Ramirez*, 141 S. Ct. 2290, 2204 (2021). Neither case requires a statutory claim have "an exact duplicate in American history and tradition." *Id.* at 2204. And as the Supreme Court confirmed, Congress may elevate to the status of legally cognizable injuries concrete, *de facto* injuries that were previously legally inadequate. *Id.* at 2204-05.

The injuries that Congress may codify and elevate include various intangible harms including "reputational harms, disclosure of private information, and intrusion upon seclusion."[2] *TransUnion*, 141 S. Ct. at 2204. With respect to intrusion upon seclusion, the Court in *TransUnion*

[2] Plaintiffs' claims are also analogous to the common-law tort of public disclosure of private information, and sufficiently pleaded to establish standing on that ground as well. *See Bohnak v. Marsh & McLennan Companies*, Inc., 79 F.4th 276 (2d Cir. 2023); *see also Davis v. Fed. Election Comm'n*, 554 U.S. 724, 733 (2008) (standing based on disclosure of private information).

cited to *Gadelhak v. AT&T Services, Inc.*, 950 F.3d 458, 462 (7th Cir. 2020), authored by now-Justice Barrett, which held that a plaintiff who received only five unwanted text messages had standing to bring a claim under the Telephone Consumer Protection Act ("TCPA"). *Id.* at 460. Judge Barrett analogized plaintiff's statutory injury to the common law tort of intrusion upon seclusion, a cause of action aimed at defendants who invade the private solitude of another. *Id.* at 462-63. Even though the common law claim would have required a "substantial" imposition on a plaintiff's privacy, Congress was free to elevate a lesser harm (here, a mere few unwanted text messages) to a legally cognizable injury. *Id.* at 462-63 ("While Congress cannot transform a non-injury on its say-so, that is hardly what it did here. Instead, Congress identified a modern relative of a harm with long common law roots."). The Court's job is to look for a close relationship "in kind, not degree." Thus, so long as the underlying *type* of harm is similar, the *quantity or extent* of the harm need not be the same. *See generally id.*[3]

The act of wiretapping or eavesdropping upon the conversations of another, without their knowledge and consent, has long been recognized under common law as one type of an intrusion

[3] *See also Drazen v. Pinto*, 74 F.4th 1336, 1339 (11th Cir. 2023)(one single unwanted text conferred standing on theory of intrusion upon seclusion); *Dickson v. Direct Energy, LP*, 69 F.4th 338 (6th Cir. 2023) (same for single unsolicited, prerecorded call to plaintiff's cell phone); *Perez v. McCreary, Veselka, Bragg & Allen, P.C.*, 45 F.4th 816, 822 (5th Cir. 2022) (courts should "focus[ ] on types of harms protected at common law, not the precise point at which those harms become actionable" (citation omitted)); *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589 (9th Cir. 2020), *cert. denied*, 141 S. Ct. 1684 (2021) (finding standing where plaintiff alleged online data tracking "*no matter how sensitive or personal users' browsing histories were*"); *Krakauer v. Dish Network, LLC*, 925 F.3d 643, 653-54 (4th Cir. 2019); *Persinger v. Sw. Credit Sys., L.P.*, 20 F.4th 1184, 1192 (7th Cir. 2021) (finding standing where plaintiff claimed intangible harm resembled a common-law intrusion upon seclusion, regardless of whether she would prevail on stand-alone common-law claim); *Lupia v. Medicredit, Inc.*, 8 F.4th 1184, 1192 (10th Cir. 2021); *Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 981 (9th Cir. 2017) (finding standing for Video Privacy Protection Act claim where ESPN disclosed Roku device serial number and identity of videos watched); *Susinno v. Work Out World Inc.*, 862 F.3d 346, 351-52 (3d Cir. 2017).

upon seclusion. *See* Restatement (Second) of Torts § 625B, cmt. b ("The invasion … may also be by the use of the defendant's senses, with or without mechanical aids, to oversee or overhear the plaintiff's private affairs, as by … tapping his telephone wires." (citing cases)); *see also Vernars v. Young*, 539 F.2d 966 (3d Cir. 1976) (recognizing a cause of action for violation of the right of privacy, including via wiretapping, under Pennsylvania common law); *Rhodes v. Graham*, 37 S.W.2d 46 (Ky. App. 1931) ("This court has adopted the rule that an unwarranted invasion of the right of privacy constitutes a legal injuria [sic] for which redress will be granted. … In short, it is the right to be let alone. … Wiretapping is akin to eavesdropping, which was an indictable offense at common law … for which the law affords a remedy by an action for damages."); *Hamberger v. Eastman*, 206 A.2d 239 (N.H. 1965) (recognizing claim for intrusion upon seclusion even though recording device placed by landlord in tenants' home never picked up sounds or voices).

Standing to bring suit in such cases has never depended on an allegation that the precise information intercepted is itself private; rather, the question is whether the plaintiff was communicating information in such a way that they believed was secure from third-party eyes or ears. *See Hamberger*, 206 A.2d 239. Defendants do not point to a single traditional wiretapping or intrusion upon seclusion case that turned on the extent to which an intercepted conversation included private information. We assume that when we pick up the phone, we are only conveying information to the person whose number we dialed. That privacy is violated when a phone is tapped. It is the act of intrusion that is offensive; not the substance of the information illegally intercepted. *See, e.g.*, *Brown v. Google LLC*, 2023 WL 5029899 (N.D. Cal. Aug. 7, 2023); *Greenley v. Kochava, Inc.,* 2023 WL 4833466, at *3 (S.D. Cal. July 27, 2023) ("Plaintiff's inability to control or prevent the unauthorized exploration of his private affairs is the root of the alleged injury") (internal quotation omitted). Likewise, when individuals sit in the privacy of their homes,

using a personal laptop or cellphone, browsing a specific website, they reasonably assume the information they convey to the website will be received by the website's owner. But individuals do not assume a third party will be, in effect, standing over their shoulder, not only watching, but *recording* every single mouse movement, click, scroll, query, and purchase. ¶¶ 64-87. The Wiretapping Statutes enacted by Congress and many of the states codify the long-held notion that the willful interception of a wire, oral, or electronic communication is an illegal act that causes a concrete injury to the person whose communication is intercepted. *See Yockey v. Salesforce, Inc.*, 2023 WL 5519323, at *3 (N.D. Cal. Aug. 25, 2023). A claim under these statutes falls squarely within the Supreme Court's standing framework articulated in both *Spokeo* and *TransUnion*.

The Third Circuit has recognized this fact when analyzing standing in the context of claims involving interception of electronic information. At least twice after *Spokeo*, the Third Circuit has examined whether plaintiffs alleging unlawful tracking of internet users' activities satisfied Article III's concrete harm requirement, both times finding standing. *See Nickelodeon*, 827 F.3d at 272-74 (website operator's intrusion on children's personal browsing and viewing activities was sufficiently injurious for purposes of standing in case brought under the Federal Wiretap Act); *In re Google Inc. Cookie Placement Cons. Priv. Litig.*, 934 F.3d 316, 325 (3d Cir. 2019) ("History and tradition reinforce that a concrete injury for Article III standing purposes occurs when Google, or any other third party, tracks a person's internet browser activity without authorization."). The outcome in this case is directly controlled by these precedents because the allegedly unlawful behavior here—surreptitious interception of internet communications—implicates the same privacy interests as those invaded by the tracking activities at issue in *Nickelodeon* and *Google.* In two additional post-*Spokeo* cases, the Third Circuit has also found that violations of federal statutes that closely relate to—but do not precisely mirror—the traditionally protected privacy right caused

concrete Article III injuries. *See In re Horizon Healthcare Servs. Inc. Data Breach Litig.*, 846 F.3d 625, 637-38 (3d Cir. 2017); *Susinno*, 862 F.3d at 351-52.[4]

The cases Defendants rely on are distinguishable or rely on an improperly broad interpretation of *TransUnion*. The courts in *Cook v. Gamestop*, 2023 WL 5529772 (W.D. Pa. Aug. 28, 2023) (currently on appeal) and *Massie v. General Motors LLC*, 2022 WL 534468 (D. Del. Feb. 17, 2022) committed a fundamental error in analyzing standing and required the privacy interests the plaintiffs alleged *be identical* to the right to privacy recognized at common law. But that is not what *Spokeo* and its progeny command—*Spokeo* asks whether the interest protected by a statute bears a "*close relationship* to a harm that has traditionally be regarded as providing a basis for a lawsuit in English or American Courts." *Spokeo*, 578 U.S. at 341. Indeed, the *Cook* and *Massie* courts' decision and Defendants' argument is in direct conflict with the Third Circuit's decision in *Google.*[5] "In an era when millions of Americans conduct their affairs increasingly

---

[4] Additionally, other federal courts have recognized that the violation of an anti-wiretapping statute is "not at all like the sort of 'bare procedural violation' that the Supreme Court has said [in *Spokeo*] would fall short of an Article III injury." *See Revitch v. New Moosejaw, LLC*, 2019 WL 5485330, at *1, 3 (N.D. Cal. Oct. 23, 2019) (holding that plaintiff had standing to assert a wiretapping claim under the California Invasion of Privacy Act ("CIPA") where the defendant utilized a software provider to eavesdrop on the plaintiff's website communications and that the "privacy harms [were] fairly traceable to the violations of California law" the plaintiff alleged); *see also Facebook Tracking*, 956 F.3d at 599; *In re Vizio, Inc. Cons. Priv. Litig.*, 238 F. Supp. 3d 1204, 1215–16 (C.D. Cal. 2017) ("While the modern contours of the tort of intrusion upon seclusion—and invasion of privacy more broadly—may not encompass the kind of detailed collection of a consumer's content viewing history alleged here, the close similarity between the conduct proscribed under the [federal] Wiretap Act and the tort of intrusion upon seclusion confirms the concreteness of Plaintiffs' injury."); *Romero v. Securus Techs., Inc.*, 216 F. Supp. 3d 1078, 1088 (S.D. Cal. 2016) Courts are particularly inclined to find a concrete invasion of privacy in the context of *surreptitious* tracking which is not reasonably known or discoverable, as Plaintiffs have alleged here. *See Hazel v. Prudential Fin., Inc.*, 2023 WL 3933073, at *5 (N.D. Cal. June 9, 2023) (surreptitious monitoring a "critical factor in deciding whether a plaintiff has plausibly pleaded that an intrusion is 'highly offensive'"); *see also Facebook Tracking*, 956 F.3d at 606.

[5] *Lightoller v. JetBlue Airways Corp.*, 2023 WL 3963823, at *4 (S.D. Cal. June 12, 2023); *Mikulsky v. Noom, Inc.*, 2023 WL 4567096 (S.D. Cal. July 17, 2023); *Straubmuller v. Jetblue Airways Corp.*,

through electronic devices, the assertion . . . that federal courts are powerless to provide a remedy when an internet company surreptitiously collects private data—is untenable. Nothing in *Spokeo* or any other Supreme Court decision suggests otherwise." *Google*, 934 F.3d at 325.

In addition, Plaintiffs here *have* alleged that the Session Replay Code captured personal information about their website visit, such as the products they searched for or purchased, for example. ¶¶ 38-52. At least two Plaintiffs allege they made website purchases, which conveyed their names, address, and billing information to the third party.[6] ¶¶ 104, 117. Plaintiffs have also alleged that SRC creates "fingerprints" that identify a user across websites for information entered on *other* websites. ¶¶ 47, 79-80. When the individual fills in his or her information on another website containing the SRC, the software can identify all other individual's sessions across other websites, even if the user had intended to remain anonymous on those other sites, including by enabling private browsing. ¶¶ 75-80. Thus, the allegations made here are more akin to those made in *In re Google*, where the defendants could compile internet histories and create detailed profiles on individuals. *See In re Google Inc. Cookie Placement Cons. Priv. Litig.*, 806 F.3d 125 (3d Cir. 2015).[7]

With respect to Plaintiffs' alleged damages, wiretapping and eavesdropping case law shows that the intrusion itself is enough, and Plaintiffs need not allege or prove mental anguish and suffering or any pecuniary damages. *See In re Google*, 806 F.3d at 134. And the cases

---

2023 WL 5671615 (D. Md. Sept. 1, 2023); *Adams v. PSP Group, LLC*, 2023 WL 5951784 (E.D. Mo. Sept. 13, 2023); and *Ann Jones v. Bloomingdales.com, LLC*, 2023 WL 6064845 (E.D. Mo. Sept. 18, 2023), are all distinguishable on the same basis.

[6] Defendant's reliance on *I.C. v. Zynga, Inc.*, 600 F. Supp. 3d 1034 (N.D. Cal. 2022) and *Brignola v. Home Properties, L.P.*, 2013 WL 1795336 (E.D. Pa. Apr. 26, 2013) are therefore also misplaced, because those cases did not involve allegations that a plaintiff's billing information was disclosed.

[7] To the extent this Court concludes that the allegations pleaded here or throughout are insufficient, Plaintiffs respectfully request the ability to amend their complaint.

Defendants cite do not involve invasion of privacy-type claims. Defendants also ignore Plaintiffs' allegations that the information surreptitiously collected from Plaintiffs has enormous monetary value to Defendants, and that Defendants are profiting from that information without Plaintiffs' prior consent to its disclosure. ¶¶ 49, 53-57. Courts have concluded that this diminution of the value of private information is actionable. *Accord Stallone v. Farmers Grp., Inc.*, 2022 WL 10091489, at *6 (D. Nev. Oct. 15, 2022). The Court should deny Defendants' 12(b)(1) motion.

B. Plaintiffs Have Standing to Seek Injunctive Relief.

To establish standing for injunctive relief, a plaintiff must demonstrate "continuing, present adverse effects." *City of Los Angeles v. Lyons*, 461 U.S. 95, 102 (1983). This standard is clearly met because Defendants continue to employ Session Replay Code that tracks all individuals that use Defendants' websites. *See Brown*, 2023 WL 5029899, at *7. This is distinguishable from data breach cases, where the injury is in the past. In addition, Defendants' argument that Plaintiffs cannot suffer harm by visiting the websites now that they know Defendants are tracking them ignores that the interception is the injury. Mere knowledge of Defendants' conduct is not consent to it, especially without an opt out. *See infra* Part II.G. If the alleged wiretap is illegal, it must be removed, or it will continue to harm Plaintiffs' and all website visitors that visit Defendants' websites. Accordingly, Plaintiffs have injunctive relief standing.

II. Plaintiffs Adequately Plead Their Wiretap Claims

A. The Party Exception to the Wiretap Statutes does not Preclude Liability.

Defendants argue that, because they were the intended recipients of Plaintiffs' communications, they are not liable for the recording of Plaintiffs' communications. MTD 7. This argument wholly misses the mark; it is the procurement of an *unknown third-party* that commits the wiretapping for which Plaintiffs complain. Simply put, as SRPs were unknown to Plaintiffs, no consent could be furnished. Because Defendants facilitated the interception of Plaintiffs'

communications by these third parties, with the intent to use that information in violation of Plaintiffs' privacy and property rights and in furtherance of unfair competition and business practices, the "party exception" does not apply.

i. CIPA Imposes Liability for Aiding the Interception of Communications

CIPA imposes liability on anyone who "aids, agrees with, employs, or conspires" with another who, "without the consent of all parties to the communication […] reads, or attempts to read […] the contents or meaning of any message, report, or communication while the same is in transit." Cal. Pen. Code § 631(a). Accordingly, Defendants are liable for inviting an "unannounced second auditor" to listen in on Plaintiffs' communications, regardless of whether Defendants consented to communicating with the third parties:

> [CIPA] expressly prohibits surreptitious monitoring without the consent of "all parties" to the conversation and specifically imposes liability on a corporation for improper eavesdropping. Under this language, [defendant] can be held liable for directing its supervisory employees to monitor confidential communications between employees and customers without properly notifying the customer about the monitoring.

Kight v. CashCall, Inc., 200 Cal. App. 4th 1377, 1393-94 (Cal. App. 2011); *Javier v. Assurance IQ, LLC*, 2023 WL 114225, at *6 (N.D. Cal. Jan. 5, 2023) (collecting cases and noting that "Section 631 concerns 'the right to control the nature and extent of the firsthand dissemination of [their] statements'"); *Yoon v. Lululemon USA, Inc.*, 549 F. Supp. 3d 1073, 1083 (C.D. Cal. 2021) ("a conversationalist is betrayed equally by a wiretapper and by the willing conversation participant who surreptitiously allows that third party to wiretap"); *Garcia v. Yeti Coolers, LLC*, 2023 WL 5736006, at *2 (C.D. Cal. Sep. 5, 2023).

While Defendants may be correct that recording their own conversation would not be prohibited by Section 631(a), Plaintiffs allege that Defendants aided unknown third parties in committing the real time interception of their browsing sessions. ¶¶ 1-4, 43, 46. Nor are the SRPs

acting merely as a "tape recorder" because "capturing, storing, and interpreting real-time data "extends beyond the ordinary function of a tape recorder." *Yoon*, 549 F. Supp. 3d at 1081; *see also Javier*, 2023 WL 114225, at *6. Because Defendants aided the SRPs' real time interception of Plaintiffs' communications, Defendants violated CIPA, irrespective of whether a party can intercept its own communications. *Valenzuela v. Nationwide Mut. Ins. Co.*, 2023 WL 5266033, at *4 (C.D. Cal. Aug. 14, 2023).

ii. Defendants Facilitated the Interception for a Tortious Purpose

Neither the Federal Wiretap Act nor the Missouri Wiretap Act recognize the party exception[8] when the interception is made for a "criminal or tortious" purpose. 18 U.S.C.A. § 2511(2)(d); Mo. Ann. Stat. § 542.402(2)(3). Illegal purposes may include "invading [a plaintiff's] privacy . . . defrauding her, or . . . committing unfair business practices." *Deteresa v. Am. Broadcasting Cos., Inc.*, 121 F.3d 460, 467 n.4 (9th Cir. 1997). Similarly, courts have found the element satisfied where a plaintiff alleged a defendant's intent to commit common law privacy violations, theft of trade secrets, or violations of state computer crime laws. *See Brown v. Google LLC*, 525 F. Supp. 3d 1049, 1067 (N.D. Cal. 2021) (violations of CIPA, intrusion upon seclusion, and invasion of privacy); *Planned Parenthood v. Ctr. for Med. Progress*, 214 F. Supp. 3d 808, 828 (N.D. Cal. 2016) (recognizing that "further invading privacy of plaintiffs' staff" sufficed to state crime-tort exception); *LMC v. ABC*, 1997 WL 405908, at *2 (D. Ariz. Mar. 27, 1997).

While a defendant must intend to commit the criminal or tortious act, a concurrent "lawful purpose" does not "sanitize" a wiretap also "made for an illegitimate purpose." *Sussman v. Am. Broad. Cos., Inc.*, 186 F.3d 1200, 1202 (9th Cir. 1999). In analyzing whether the interception was

[8] Separate and apart from the party exception, the Missouri statute prohibits "us[ing] […] the contents of any wire communication, when he knows or has reason to know that the information was obtained through the interception of a wire communication[…]. Mo. Ann. Stat. § 542.402.

in furtherance of a criminal or tortious act, a court looks not to the means of interception (*i.e.*, not whether the interception was prohibited), but the reason for undertaking the interception (*i.e.*, what the defendant intended to gain from the interception). *See In re DoubleClick Inc. Priv. Litig.*, 154 F. Supp. 2d 497, 516 (S.D.N.Y. 2001) (citing *Sussman*, 186 F.3d at 1202). "It is the use of the interception with *intent to harm* rather than the fact of interception that is critical to liability." *Boddie v. ABC*, 881 F.2d 267, 270 (6th Cir. 1989). Accordingly, the party exception cannot be applied as a matter of law where the plaintiff alleges the interception was conducted "for the purpose of invading her privacy[.]" *In re DoubleClick Inc. Priv. Litig.*, 154 F. Supp. 2d at 516 (quoting *Deteresa*, 121 F.3d at 467 n.4).

Here, Plaintiffs have alleged exactly that. By facilitating the SRPs' interception, Defendants intended to invade Plaintiffs' privacy rights and reappropriate their information to Defendants' own pecuniary benefit. ¶¶ 3, 31-36. Defendants realize this pecuniary benefit by sending targeted advertisements to Plaintiffs and by using their information to glean valuable performance and analytical insights. ¶¶ 31, 53-57, 125, 183. And Plaintiffs allege that this practice constitutes unfair competition injuring both themselves and Defendants' competitors who do not realize such a pecuniary advantage. ¶¶ 43, 49, 250. Because Plaintiffs have alleged that Defendants facilitated the interception for the purpose of invading their privacy, committing unfair business practices, and converting their personal and private information to Defendants' own pecuniary benefit, they have satisfied their burden at this stage. *See Bowens v. Aftermath Ent.*, 254 F. Supp. 2d 629, 644 n.5 (E.D. Mich. 2003) ("So long as Plaintiffs have alleged at least one 'tortious purpose,' the prior consent exception is not available to Defendants as grounds for dismissal.").

Defendants attempt to impose a heightened standard on the criminal or tortious conduct element of the party exception by asking the Court to require not just that Defendants intended to

commit a tort but "that Defendants intended to use the allegedly intercepted information for a criminal or tortious purpose." MTD 10. But they cite no authority for that proposition. Nevertheless, even if the tortious conduct must result from Defendants' use of intercepted communications, Plaintiffs allege that Defendants intended to acquire the information for its value in delivering targeted advertisements to Plaintiffs, tracking them across websites, and analyzing their browsing sessions after the fact. ¶¶ 3, 31-32, 35-36, 46 ("[The intercepted information] was later used by Defendants, and by third parties, to facilitate their own products and services for financial gains."), 49, 80.

And to the extent Defendants argue that they cannot invade the privacy of a fellow conversation participant, an individual maintains a reasonable expectation of privacy even when they are aware that the other party to a conversation may intercept the communication. *Huff v. Spaw*, 794 F.3d 543, 554 (6th Cir. 2015) ("[S]omeone who knowingly converses with a person who may be carrying an interception-capable device can nonetheless enjoy a reasonable expectation of privacy from interception."); *see supra* Part I.A.

B. Plaintiffs Adequately Allege Interception of "Contents" under the Federal, California, Maryland, Massachusetts, and Pennsylvania Acts.

Plaintiffs plausibly allege that Defendants intercepted the "substance, purport, or meaning" of their electronic communications. ¶¶ 65, 69, 97-99, 103-105, 109-118, 123, 128, 133, 140-147. As one court held:

> FullStory captures mouse movements, clicks, typing, scrolling, swiping, tapping, keystrokes, geographic location, IP addresses, and data entry . . . FullStory records these and other details alongside "a video capturing each of Plaintiff's keystrokes and mouse clicks on the website" . . . Although not all of this information may constitute the "contents" of a communication under the federal Wiretap Act, Plaintiff has met his burden to allege facts plausibly showing Defendants recorded Plaintiff's content communications with Nike by recording, among other things, keystrokes and a video of Plaintiff's interactions with Nike's website.

Saleh v. Nike, Inc., 562 F. Supp. 3d 503, 517-18 (C.D. Cal. 2021).[9]

In applying the Federal Wiretap Act and other wiretapping statutes, courts distinguish between contents of a communication and "record information" associated with the communication. *See S.D. v. Hytto Ltd.*, 2019 WL 8333519, at *6 (N.D. Cal. May 15, 2019). "[P]rotected 'content' under the Act is a person's 'intended message to another.'" *Id*. (quoting *In re Zynga Priv. Litig*., 750 F.3d 1098, 1098 (9th Cir. 2014)). Ultimately, the distinction lies in the automatic nature of record information: "[u]nlike record information, content is generated not automatically, but through the intent of the user." *Id*. (citing *In re iPhone App. Litig.*, 844 F. Supp. 2d 1040, 1041 (N.D. Cal. 2012)). As a result, the *type* of information collected is not as determinative as the *context* by which it was generated under a "contents" analysis. *See In re Google*, 806 F.3d at 137 (noting that an "address, phone number, or URL" is "part of the substantive information conveyed" it is "content," and inquiry "is a case-specific one turning on the role the location identifier played in the 'intercepted' communication").

Courts analyzing intercepted communications have consistently held that an individual's intent is reflected by their interactions with a website and is therefore considered content. *See e.g. Brown*, 525 F. Supp. 3d at 1056 (finding content where user initiated exchange of HTTP requests and responses from online interactions "enables Google to learn exactly what content the user's browsing software was asking the website to display"); *see also Brown*, 2023 WL 5029899, at *15 (denying summary judgment); *Facebook Tracking*, 956 F.3d at 605 (URLs and browsing history

[9] As Defendants note (MTD 11), "contents" is defined consistently across all relevant jurisdictions to which this argument applies. As relevant, Plaintiffs allege violations of the Federal Wiretap Act (Count I), CIPA (Count III), the Maryland Wiretapping and Electronic Surveillance Act ("MWESA") (Count VI), the Massachusetts Wiretapping Statute ("MWS") (Count VIII), and the Pennsylvania Wiretapping and Electronic Surveillance Control Act ("WESCA") (Count XIII).

are content because they could "divulge a user's personal interests, queries, and habits[.]"); *In re Google*, 806 F.3d at 137-38 (URL addresses considered content when generated by user interaction and noting "[t]he line between contents and metadata is not abstract but contextual with respect to each communication"); *In re Google RTB Cons. Priv. Litig.*, 606 F. Supp. 3d 935, 949 (N.D. Cal. 2022) (website categories, categories that describe the current section of the website, and referrer URL causing navigation to the current page constituted "content"); *Doe v. Meta Platforms, Inc.*, 2023 WL 5837443, at *4 (N.D. Cal. Sept. 7, 2023) (contents include log-in buttons and URLS including "query string"); *Alves v. BJ's Wholesale Club, Inc.*, 2023 WL 4456956, at *4 (Mass. Sup. Ct. June 21, 2023) ("keystrokes, clicks, mouse movements, URLs, and other data" considered "content"); *Vasil v. Kiip, Inc.*, 2018 WL 1156328, at *3-4 (N.D. Ill. Mar. 5, 2018) (adopting Third Circuit framework to determine geo-locational data constitutes contents).

Plaintiffs' Complaint describes, *at the very least*, an array of content sufficient to satisfy the fact-intensive standard applied to the "contents" analysis under the pleaded wiretapping acts. The electronic communications captured through Defendants' procured Session Replay Code was content generated through Plaintiffs' intended use, interaction, and communication with Defendants' websites, conveying the substance and/or meaning of Plaintiffs' communications with the websites, *i.e.*, what they searched for, bought, viewed, or engaged with. ¶¶ 73, 90-91, 97-99, 103-105, 109-111. The data obtained allowed Defendants and third parties to capture, observe, and divulge Plaintiffs' personal interests, search queries, and habits, and thus revealed personalized and sensitive information about Plaintiffs. ¶¶ 151, 266, 282-283, 308, 325-326. As the Complaint screenshots support, the communications included detailed accounts of Plaintiffs' intentional interactions with the websites, including descriptive URLs for items clicked on and which stores Plaintiffs researched. ¶¶ 140-141. This data was solely created by Plaintiffs through their intended

interactions with the websites, such that it "divulge[d] [their] personal interests, queries, and habits[.]" *Facebook Tracking*, 956 F.3d at 607. Plaintiffs' communications were not automatically generated or incidental; they reflected specific intent and contained content that was generated by Plaintiffs through their communicative interactions with Defendants' websites. As such, Plaintiffs have sufficiently alleged the "contents" of their communications were intercepted.

C. Plaintiffs' Communications Were Intercepted Contemporaneously with Transmission.

Misconstruing the well-pleaded allegations in the Complaint, Defendants argue that Plaintiffs fail to allege contemporaneous "interception" under the Federal Wiretap Act, CIPA, or MWESA. MTD 14-15. But the Complaint specifically and sufficiently alleges and describes how the Session Replay Code procured and employed by Defendants "contemporaneously intercept[s]" virtually every user action with Defendants' website. *See, e.g.*, ¶ 5, 6, 67, 267, 269.

Defendants rely on a misreading of a single, cherry-picked allegation in the Complaint. MTD 15 (quoting ¶ 68). In fact, the "intervals" Defendants argue are sequential are contemporaneous and transmitted "milliseconds apart" "throughout the user's website session, rather than after the user's visit to the website is completely finished." ¶ 68. Defendants may not manufacture grounds for dismissal by ignoring and misconstruing allegations.

Defendants' case law supports Plaintiffs' interpretation. In *Martin v. State* , the Maryland Court of Special Appeals specifically distinguished between cases where "acquired communications were in storage at the time of their acquisition" and "the interception of messages transmitted over [] communications networks[] [that] . . . rely upon subdivision of a digital message into smaller 'packets,' each of which is sent separately and independently (and perhaps over a different pathway) and ultimately re-assembled[.]" 96 A.3d 765, 775 n.23 (Md. App. 2014) (explaining "the messages at issue had been received hours before the police had obtained access

to them, and their storage, for an indefinite duration . . . is of an entirely different character than the transient storage of 'packets' in the memory of routers during transit."). Numerous courts have consistently held that the transmission of communications facilitated by website tracking technologies, including SRC, occurs contemporaneously. *See e.g. Garcia*, 2023 WL 5736006, at *4; *Valenzuela*, 2023 WL 5266033, at *5 (allegations of interception "in real time" and details on how it occurs sufficient at the pleadings stage); *Hazel*, 2023 WL 3933073, at *3 (same); *see also United States v. Szymuszkiewicz*, 622 F.3d 701, 706 (7th Cir. 2010); *In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 102-28 (N.D. Cal. 2014). The Complaint more than adequately alleges how the "contemporaneous interception" of Plaintiffs' communications occurred to justify motion denial.

D. Session Replay Code Is a "Device" under MWESA, MWS, and WESCA.

Defendants argue that Plaintiffs' claims under MWESA, MWS, and WESCA should be dismissed because software cannot be a device. Defendants' argument fails for two reasons. First, contrary to Defendants' hyper-technical statutory reading, "device" is not limited to something tangible. Second, courts have routinely found that software can be a device for purposes of a wiretapping statute. *See, e.g.*, *Doe*, 2023 WL 5837443, at *7 (finding that software embedded on a website, the Meta Pixel, is a device under CIPA); *United States v. Hutchins*, 361 F. Supp. 3d 779, 795 (E.D. Wis. 2019) ("Section 2510(5)'s reference to 'mechanism,' which is commonly defined as a 'process, technique, or system for achieving a result' seems to encompass software."); *Luis v. Zang*, 833 F.3d 619, 634 (6th Cir. 2016) ("WebWatcher is a device specifically designed to surreptitiously "intercept[ ] communications"); *United States v. Barrington*, 648 F.3d 1178, 1203, (11th Cir. 2011) (accepting keylogger software as a "device" under Federal Wiretap Act); *In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051, 1084 (N.D. Cal. 2015) ("Plaintiffs have sufficiently alleged that the Carrier IQ Software is a 'device' for purposes of the Wiretap Act."); *Klumb v. Goan*, 884 F. Supp. 2d 644, 661 (E.D. Tenn. 2012). Additionally, Plaintiffs allege that even if the software is

not a device, the SRC alters the operation of Plaintiffs' phones and computers, which are themselves tangible devices. ¶ 150.

Maryland. Under MWESA, "electronic, mechanical or other device" is not limited to something "tangible." MWESA's "clear purpose" is to prohibit the secret recordings of private communications "without regard to which device may be used to accomplish the task . . . . nothing in the language or purpose of the statute [ ] distinguish[es] secret recordings made with the devices of yesteryear" from those made with modern technology. *Holmes v. State*, 182 A.3d 341, 350-51 (Md. App. 2018) (finding a smartphone app used to record a conversation is considered a "device" under MWESA).

This conclusion is consistent with MWESA's statutory definitions. Under MWESA, "intercept" is defined as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of ***any*** electronic, mechanical, or other device." Md. Code Ann., Cts. & Jud. Proc. § 10-401(10). The use of the word "any" before "electronic, mechanical, or other device" in Section 10-401(10) implies that the class of technology contemplated by MWESA is broader than just tangible items. *See Any*, Merriam-Webster Dictionary, https://www.merriam-webster.com/dictionary/any#dictionary-entry-1 ("used to indicate one selected without restriction"). Despite this broad meaning, Defendants improperly attempt to read out "any" and "electronic" by limiting "device" to something tangible. This violates a basic canon of statutory construction. *See Mid-Atl. Power Supply Ass'n v. Pub. Serv. Comm'n of Md.*, 760 A.2d 1087, 1097 (Md. App. 2000).

The case law Defendants rely upon in support of their misguided interpretation is unpersuasive. *See Mason v. Mach. Zone, Inc.*, 140 F. Supp. 3d 457 (D. Md. 2015), *aff'd*, 851 F.3d 315 (4th Cir. 2017) (concluding that a smart phone app was not a "slot machine or device" under

a California law that narrowly defined "slot machine or device" as a "machine, apparatus, or device" such that it was limited to a "piece of equipment."); *compare Cavanaugh v. State*, 2020 WL 3485717, at *4 (Md. App. June 26, 2020) (concluding that where an individual recorded a phone call with an application installed on his cell phone, he "acquired the contents of a wire communication through the use of an electronic device" under MWESA).

Massachusetts. Without citation to case law, Defendants declare that an "intercepting device" under MWS is also limited to something tangible. MTD 17. However, MWS broadly defines "intercepting device" to include: "any device or apparatus which is capable of transmitting, receiving, amplifying, or recording a wire or oral communication." Mass. Gen. Laws ch. 272, §99(B)(3). Indeed, a Massachusetts court rejected this exact argument and concluded that SRC was an intercepting device. *See Alves*, 2023 WL 4456956, at *5; *see also Rich v. Rich*, 2011 WL 3672059 at *6 (Mass. Super. July 8, 2011) (key logger software was an intercepting device because it could record wire communications).

Pennsylvania. Defendants' argument that a "device" under WESCA is limited to something tangible is contradicted by plain language and precedent. "WESCA defines the term 'device' broadly" and "exceptions to WESCA's definition of 'device[]' must be construed narrowly." *Popa v. Harriet Carter Gifts, Inc.*, 426 F. Supp. 3d 108, 116 (W.D. Pa. 2019). Under WESCA, "device" is defined as "[a]ny device or apparatus . . . that can be used to intercept a wire, electronic or oral communication." 18 Pa. C.S.A. § 5702. In turn, "electronic communication" is defined as "any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo-optical system." 18 Pa. C.S.A. § 5702. "[T]he relationship between these two definitions [device and electronic communications] is critical to the analysis." *Popa*, 426 F. Supp. 3d at 117. Furthermore,

the use of the word "any" "implies that the class of technology contemplated by WESCA is broad." *Id.*; *see, e.g.*, *Commonwealth v. Smith*, 136 A.3d 170, 178 (Pa. Super. 2016) (software app on smartphone is an interception "device" under the WESCA).

While Pennsylvania courts have not decided whether software constitutes a device, they have held that whether something is a "device" is a question of fact better addressed after discovery. *See Harriet Carter*, 426 F. Supp. 3d at 117; *Oliver v. Noom, Inc.*, ECF 28 at 13 (W.D. Pa. Aug. 22, 2023) (explaining that "[a]s alleged," Noom's SRC "could reasonably be considered a 'device or apparatus'" and discovery would allow "the opportunity to develop a factual record").

The plain language of the statutes and the relevant case law interpreting those definitions forecloses Defendants' attempt to limit a "device" under MWESA, MWS, and WESCA to something tangible, and this Court should reject them.

E. Session Replay Code is Not "Telephone Equipment" Exempted by MWESA

MWESA's "telephone exception" exempts "telephone equipment" used in the "ordinary course of business" from the definition of wiretapping devices (*see* Md. Code Ann., Cts. & Jud. Proc. § 10-401(8)), but "the default rule is that the device is an intercepting device forbidden by the Maryland Wiretap Act." *Schmerling v. Injured Workers' Ins. Fund*, 795 A.2d 715, 726-27 (Md. 2002) ("[T]he statutory exception to this blanket prohibition is for telephone equipment . . . used in the ordinary course of business. Both criteria must be met to satisfy the 'telephone exemption[.]'"). Here, SRC procured and employed by Defendants does not facilitate or enhance the exchange of communicative requests and responses through the Hypertext Transfer Protocol – the method of communication at issue here. ¶ 66. Therefore, it is not "telephone equipment."

Defendants' argument is predicated on misconstruing the holding in *Schmerling* to argue that since communications occur on Defendants' websites, and Defendants derive benefits from

SRC, it therefore meets the exemption. MTD 19. However, to qualify for the exemption, SRC must "further the use of or functionally enhance the []communications system." *Schmerling,* 795 A.2d at 716-17. In *Schmerling*, the Maryland Court of Appeals made clear that "the exemption only applies if the equipment is telephone equipment . . . or a component thereof." *Id*. (internal quotation marks omitted); *see also Cavanaugh*, 2020 WL 3485717, at *5. The device at issue in *Schmerling* was a telephone monitoring and recording system, procured by the defendant from a third-party provider that "enable[d] the recording of calls made to and from individual telephone lines." 795 A.2d at 717. The court nonetheless concluded that this system did not constitute "telephone equipment" for purposes of the telephone exemption because it did not contribute to the "facilitation of communication" through the telephone system. *Id.* at 726-27.

Here, Defendants argue SRC "simply helps Defendants communicate with their website visitors, and helps visitors effectively communicate with Defendants. As a result, Defendants' session replay software furthers 'the use of or functionally enhance[s] [Defendants'] telecommunications system.'" MTD 19. Defendants' exact argument was rejected in *Schmerling*, where "[i]t [was] undisputed that the [defendant's] purpose for installing the [] monitoring system was to evaluate and improve customer service." 795 A.2d at 717-18. The court concluded that it did not enhance the facilitation of communication because it "[did] nothing other than monitor and record[.]" *Id.* at 727 ("[T]he telecommunications equipment itself was not improved, enhanced, or furthered by the addition of the monitoring and recording devices."). The same is true here. SRC does not itself enhance or even relate to the facilitation of telecommunication, *i.e.*, the actual transmission of the originating communications. Instead, it is a "'a device placed on the line in order to receive the communication during its transmission'" and, as such "it is precisely the type of device intended to be restricted under the wiretapping statutes." *Id*. at 726-27.

Like the respondents in *Schmerling*, Defendants incorrectly "believe that so long as a device is made and sold commercially, connected directly to the [telecommunications system] and deeply integrated into the users [telecommunications] system, it should be considered telephone equipment or a component thereof.… Such a standard, however, would render the first prong a virtual nullity… This is certainly not what the Legislature intended." *Id*. And like the telephone monitoring system in *Schmerling*, the SRC "does nothing other than monitor and record". *Id*. It does not facilitate or enhance HTTP communications; it surreptitiously intercepts them for Defendants' benefit.[10] Accordingly, "the exemption cannot apply." *Id.*

F. Session Replay Code Is Not a Tracking Device Under WESCA.

Defendants argue that even if SRC is deemed a "device" under WESCA, it is a "tracking device" and therefore exempt from WESCA's prohibitions. This is an unconstrained reading of "tracking device." Indeed, federal courts analyzing a similar definition of "tracking device"[11] under the Federal Wiretap Act (18 U.S.C. § 2510(12)(C); 18 U.S.C. § 3117(b)) have concluded that the term merely "incorporated the then-common understanding of tracking device, to wit: a device designed and intended to perform a law enforcement function of tracking an automobile, person or item after being 'placed' by agents." *In re Smartphone Geolocation Data App.*, 977 F. Supp. 2d 129, 149 (E.D.N.Y. 2013). Put differently, a "tracking device" contemplates devices of the "beeper" variety, *i.e.*, "one-way radio communication devices that emit a signal on a specific radio frequency." *In re App. for an Ord. Authorizing the Extension & Use of a Pen Reg. Device*, 2007 WL 397129, at *2 (E.D. Cal. Feb. 1, 2007). WESCA was modeled after the Federal Wiretap Act; this Court can thus look to federal court "tracking device" interpretations. *Com. v. Deck*, 954

[10] This is also a fact question inappropriate for resolution at a motion to dismiss.
[11] WESCA is further restrictive than the federal counterpart because it contains the word "only."

A.2d 603, 607 (Pa. Super. Ct. 2008). As a result, it is clear that SRC—which is software that captures and collects content of communications—is not a physical tracking device used to track cars, persons, or items. *See Commonwealth v. Glass*, 200 A.3d 477, 488 (Pa. Super. Ct. 2018) (criminal informant's transmitter recorder which recorded audio and included location for informant safety was not a "tracking device" because it was not a GPS device police attached to suspect's vehicle).

The Florida cases Defendants rely on are unpersuasive. The *Jacome* court hardly engaged in a rigorous analysis, reaching its conclusion in a mere sentence. *Jacome v. Spirit Airlines Inc.*, 2021 WL 3087860, at *5 (Fla. Cir. Ct. June 17, 2021). Defendants' argument from *Goldstein v. Costco Wholesale Corp.*, 559 F. Supp. 3d 1318, 1321 (S.D. Fla. 2021), that the detailed information collected is akin to that recorded by a brick-and-mortar store security camera has been rejected as flawed. *See Moosejaw*, 2019 WL 5485330, at *1 ("[A] customer in brick-and-mortar store does not communicate by searching through the inventory. But the same is not true for off-site shoppers: a customer who calls to inquire about a store's products undoubtedly communicates with the retailer. As does an online patron."). Given the detailed information collected by SRC and the dearth of legal analysis here, this Court need and should not follow non-binding, out-of-circuit precedent. "Exceptions to WESCA's definition of 'devices' must be construed narrowly and none of them seemingly apply here." *Harriet Carter*, 426 F. Supp. 3d at 117.

G. Plaintiffs did not consent to Defendants' use of Session Replay Code.

Defendants contend that Plaintiffs' Wiretap Claims should all be dismissed because Defendants maintain a Privacy Policy[12] that allegedly discloses their use of Session Replay and

[12] Defendants purport to maintain a singular "Privacy Policy" across both www.basspro.com and www.cabelas.com. ¶ 155. Herein, "Privacy Policy" refers to the policy on both websites.

establishes users consented to being tracked by SRC. Def. Br., at 24. Posting an unenforceable browsewrap Privacy Policy on the bottom of a website in small low-contrast font, however, does not manifest users' consent. But Defendants' argument fails for two additional, independent, reasons. First, the interception occurs the moment a website visitor interacts with Defendants' websites, providing no time to review the Privacy Policy before the wiretapping occurs. ¶¶ 64-74; 153-56. Defendants cannot overcome this significant hurdle, as "*[p]rior consent* is a complete defense," but subsequent consent is not. MTD 21; *Javier v. Assurance IQ, LLC*, 2022 WL 1744107, at *2 (9th Cir. May 31, 2022) (rejecting the proposition that a website user can subsequently provide consent to a wiretapping by responding to a prompt on the same website which is already being wiretapped); *see also Cothron v. White Castle Sys., Inc.*, 2020 WL 3250706, at *6 (N.D. Ill. June 16, 2020); *cf. Kauders v. Uber Techs., Inc.*, 2019 WL 510568, at *5 (Mass. Super. Ct. Jan. 3, 2019) (plaintiff did not consent to arbitration where the terms were not disclosed until after the plaintiff created an account). Any purported notice and consent concerning the wiretapping on Defendants' websites could not have happened until after the Plaintiffs had already been wiretapped. ¶¶ 153-55.

Moreover, Defendants improperly raised their consent defense in its Rule 12(b)(6) motion, and the Court should deny it as premature. *See Doe v. Smith*, 429 F.3d 706, 709 (7th Cir. 2005) (finding "[c]omplaints need not anticipate or attempt to defuse potential defenses," … "the defense of single-party consent has limits," and reasoning that plaintiff may be able to show a crime-tort purpose); *Doe*, 2023 WL 5837443, at *5 (consent is an "evidence-bound determination[]" "inappropriate to reach on this motion [to dismiss]").

Dispositively, though, Defendants have the burden to establish consent and have failed. *See Brown*, 525 F. Supp. 3d at 1063 (burden on defendant); *accord Brown*, 2023 WL 5029899, at

*7 (denying summary judgment on consent defense). "Consent must be actual," which requires a disclosure that "explicitly notif[ies]" users of the practice at issue. *Id.*; *In re Facebook, Inc., Cons. Priv. User Profile Litig.*, 402 F. Supp. 3d 767, 789-90 (N.D. Cal. 2019) ("[I]f a reasonable ... user could have plausibly interpreted the contract language as not disclosing that [the defendant] would engage in particular conduct, then [the defendant] cannot obtain dismissal of a claim about that conduct (at least not based on the issue of consent).") Defendants have not met their burden here because they never disclosed (1) the existence of the Privacy Policy or acquired Plaintiffs' assent to its terms; or (2) their interception of private browsing communications using SRC.[13]

i. Defendants' Privacy Policy is an Unenforceable Browsewrap Agreement.

Defendants' Privacy Policy is an unenforceable browsewrap agreement, and there is no evidence suggesting that Plaintiffs had fair notice of the "terms" of using Defendants' website before the wiretapping began (which is instantaneous upon arriving on Defendants' websites). Agreements on the internet are either "clickwrap" or "browsewrap" agreements. *See James v. Glob. TelLink Corp*, 852 F.3d 262, 267 (3d Cir. 2017). "Unlike online agreements where users must click on an acceptance after being presented with terms and conditions (known as 'clickwrap' agreements), browsewrap agreements do not require users to expressly manifest assent." *Id.*; *see also Nguyen v. Barnes & Noble Inc.*, 763 F.3d 1171, 1177 (9th Cir. 2014). In browsewrap agreements, a company's policies are generally posted via hyperlink at the bottom of the webpage. *Glob. TelLink*, 852 F.3d at 267. While clickwrap agreements are "routinely enforced by the courts," *HealthPlanCRM LLC v. AvMed, Inc.*, 458 F. Supp. 3d 308, 334 (W.D. Pa. 2020), browsewrap agreement's "often turn[] on whether the terms or a hyperlink to the terms are

[13] Additionally, Plaintiffs' consent is irrelevant because Defendants intercepted Plaintiffs Website Communications with the intent to commit a criminal or tortious act. *See supra* Part II.A.

reasonably conspicuous on a webpage." *Glob. TelLink*, 852 F.3d at 267; *see also McDaid v. Avant, LLC*, 2021 WL 9803613, at *1 (W.D. Pa. Oct. 26, 2021). Whether someone has inquiry notice of a browsewrap agreement turns on the design of the website, and whether the link to the browsewrap agreement "is buried at the bottom of the page or tucked away in obscure corners of the website where users are unlikely to see it," and if so, "courts have refused to enforce the browsewrap agreement." *Nguyen*, 763 F.3d at 1177 (internal citations omitted); *see also Specht v. Netscape Commc'ns Corp.*, 306 F.3d 17, 23 (2d Cir. 2002); *In re Zappos.com, Inc., Customer Data Sec. Breach Litig.*, 893 F. Supp. 2d 1058,1064 (D. Nev. 2012); *Hines v. Overstock.com*, 668 F. Supp. 2d 362, 367 (E.D.N.Y. 2009), *aff'd*, 380 F. App'x 22 (2d Cir. 2010).

Defendants' purported Privacy Policy does not require affirmative consent, rendering it a browsewrap agreement that is only valid if Plaintiffs had actual or constructive notice of its terms and conditions. *Glob. TelLink*, 852 F.3d at 267. [14] Here, Plaintiffs allege they had no inquiry or actual notice of the terms; the Privacy Policy is contained on the homepage in small low-contrasting font at the bottom of the page. ¶ 155. Nothing about the Privacy Policy was conspicuous and Plaintiffs alleged they were never prompted to look at it. ¶¶ 101, 107, 113, 120, 125, 130, 135, 155. Thus, Plaintiffs sufficiently allege that the terms of the privacy policy are not conspicuous, and therefore unenforceable. *See Glob. TelLink*, 852 F.3d at 267; *see also Nguyen*, 763 F.3d at 1177.

Defendants offer no evidence indicating that Plaintiffs would have been unable to navigate Defendants' website until they were on inquiry notice of Defendants' purported Privacy Policy.

[14] Defendants' citation to *Silver v. Stripe, Inc.*, 2021 WL 3191752 at *4 (N.D. Cal. July 28, 2021) is thus inapposite, as the court found that defendant there utilized a "sign-in wrap" agreement, which required plaintiffs to affirmatively agree to defendants' terms of service and privacy policy.

Instead, Defendants argue that merely visiting a website that contains a privacy policy is sufficient to furnish prior consent.[15] The Ninth Circuit has rejected similar arguments. *See Javier*, 2022 WL 1744107, at *2. In any event, given the inherent fact issues of whether the Privacy Policy provides actual or inquiry notice of wiretapping, Defendants' consent argument at the pleadings stage cannot overcome Plaintiffs' well-pleaded allegations. This Court should reject Defendants' argument outright, or reserve judgment on this issue until after discovery. *See Putt v. TripAdvisor Inc*., 2021 WL 242470, at *7 (E.D. Pa. Jan. 25, 2021).

ii. The Privacy Policy did not disclose Session Replay Code or Providers

Even assuming users consented to the Privacy Policy, the argument still fails because the Privacy Policy did not specifically disclose Defendants' use of session replay tracking. *See Brown*, 525 F. Supp. 3d at 1064 (finding no consent because the policy provisions did not explicitly address the alleged unlawful conduct); *see also McCoy v. Alphabet, Inc.*, 2021 WL 405816, at *4 (N.D. Cal. Feb. 2, 2021) ("[C]onsent is only effective if the person alleging harm consented to the particular conduct[.]"); *Opperman v. Path, Inc*., 205 F. Supp. 3d 1064, 1074 (N.D. Cal. 2016) ("[I]t is unclear whether . . . the relevant Privacy Policy provisions even [regard the] function at issue in the lawsuit.").

The Privacy Policy uses vague, undefined terms to describe Defendants' conduct. Defendants' Privacy Policy purportedly states they: "may use third party-placed tracking pixels

[15] Defendants also argue that Plaintiffs knew or should have known they were being recorded on Defendants' websites simply because they were using the internet. MTD 21, 25 (citing *Commonwealth v. Byrd*, 235 A.3d 311, 319 (Pa. 2020) and *Commonwealth v. Proetto*, 771 A.2d 823, 829 (Pa. Super. 2001), *aff'd*, 837 A.2d 1163 (Pa. 2003)). These cases do not stand for an automatic assumption of recording on the internet. Rather, they concern a conversation in prison over a closed-circuit telephone that clearly indicated "this call may be monitored or recorded," and messages sent via emails and chat rooms, respectively. Both fact patterns establish situations where a person would know they were being recorded. *See also supra* Part I.A., *infra* III.B.

and Cookies," collect "browsing or search history, website interactions, and advertisement interactions," and disclose that information to "service providers and others, such as advertising and analytics partners; affiliated companies; law enforcement." MTD 22-23. This is not sufficient disclosure to put users on notice of use of SRC. Importantly, it does not indicate that third parties collect this information in real time. Rather, at best, the Privacy Policy indicates that Defendants will collect it, then share it at a later date (which would not violate the wiretapping statutes). "Even if a privacy statement discloses some kinds of tracking, a defendant can still be liable for other kinds of tracking that the privacy statement does not disclose." *Harriet Carter*, 426 F. Supp. 3d at 118 (citing *In re Yahoo*, 7 F. Supp. 3d at 1028).

SRC intercepts and captures the content of individuals' Website Communications in a manner that is far more active and invasive than other analytics tools like cookies, tags, or web beacons. ¶¶ 5, 151, 310; *see also Alves*, 2023 WL 4456956, at *5 (SRC is "significantly different" from cookies). Also, the terms "browsing history" and "website interactions" do not convey real-time recording of a user's "every move on a website," as SRC operates. ¶¶ 65, 87, 91. Indeed, SRC is sophisticated computer software that allows Defendants and third-party SRPs to contemporaneously intercept, view, and capture users on the website in real-time, "including capturing partial text field submissions that users did not intend to send to Defendants (for example, by closing the browser before hitting 'submit'), and certainly did not intend to send to third-party Session Replay Providers." ¶¶ 1, 7, 259, 268, 299, 312, 342, 405. Vague references to "cookies" and "website interactions" are insufficient to disclose the invasive, and all-encompassing tracking occurring when SRC is deployed on Defendants' websites. Additionally, "[t]hat the person communicating knows that the interceptor has the capacity to monitor the communication is insufficient to establish implied consent." *In re Google Inc.,* 2013 WL 5423918,

at *12 (N.D. Cal. Sept. 26, 2013); *see also Watkins v. L.M. Berry & Co.,* 704 F.2d 577, 581 (11th Cir. 1983) ("[K]nowledge of the capability of monitoring alone cannot be considered implied consent."). Defendants' statements *they* "may" collect user information cannot support dismissal based on consent.

In sum, Defendants' Privacy Policy does not establish consent to the secret tracking occurring on Defendants' websites, and Defendants fail to meet their burden to justify dismissal.

III. Plaintiffs Sufficiently Plead Claims for Invasion of Privacy.

Plaintiffs bring claims for intrusion upon seclusion under the common law of Maryland, Massachusetts, Missouri, and Pennsylvania. ¶¶ 276-96, 318-39, 382-402, 422-41.[16] The central issues are consistent across the states: (1) the offensive nature of the intrusion; and (2) the protected privacy interest infringed. *See* Restatement (Second) of Torts § 652B ("One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person."). Plaintiffs properly plead the predicates required.

A. Plaintiffs allege an intentional intrusion into their privacy.

Defendants argue that Plaintiffs fail to adequately allege intent. MTD 26. However, Plaintiffs included substantial allegations that Defendants had the option to be less intrusive, but chose to take the more intrusive application of the session replay technology. *E.g.*, ¶¶ 7, 32, 69 (Defendants decline to use available masking configuration settings and transmit all the captured

[16] Massachusetts has codified the common law right to be free from invasions of privacy in Mass. Gen. Laws ch. 214 § 1B. *Polay v. McMahon*, 10 N.E.3d 1122, 1126 (2014) ("[A] plaintiff . . . may support a claim of invasion of privacy by showing that a defendant has intruded unreasonably upon the plaintiff's 'solitude' or 'seclusion.' The right which the plaintiffs claim was infringed upon is their right to be left alone.") (internal citations and quotations omitted).

data to SRPs"), 312 ("Defendants intentionally procure and embed [SRC] on their websites to spy on, automatically and secretly, and intercept" visitor communications, "without their consent and in real-time."); *see also* ¶¶ 330, 432. Defendants' intrusion and de-anonymization of Plaintiffs' communications is not accidental; this is an intentional feature, not a bug.

McCauley v. Suls, 123 Md. App. 179, 190 (Md. App. 1998), illustrates the difference between cases that found negligent intrusions, which are not actionable, from this intentional intrusion. In *Suls,* counsel issued subpoenas without notice to opposing counsel, but fact discovery uncovered no evidence the failure was intentional. *Id.* at 183. In addition, the subpoenas were neither an unreasonable intrusion nor was there anything more than conjecture regarding intent. *Id.* Here, however, Defendants purposefully use SRC to surreptitiously record a person's actions, to look over their shoulder and unmask their identity, for marketing, tracking and other monetary purposes. Defendants choose to intentionally and unreasonably intrude.

B. Plaintiffs had a reasonable expectation of privacy.

Defendants argue Plaintiffs have no reasonable expectation of privacy in information Plaintiffs shared on their websites. MTD 27. First, this dramatically misunderstands the nature of eavesdropping and the privacy injury, as explained above. *See supra* Part I.A. Defendant also conveniently ignores the pleadings related to information not intentionally shared, and the de-anonymizing nature of the technology employed. *See, e.g.*, ¶¶ 74, 79-80, 101, 107, 120, 125, 130, 135, 142-48, 153-57. At the very least, Plaintiffs had a reasonable expectation of privacy in information they did not intend to share, fingerprinting between websites, and de-anonymizing them. Courts also routinely find that plaintiffs have a reasonable expectation of privacy in their interactions with websites online. *See, e.g.*, *Facebook Tracking*, 956 F.3d at 604 n.7 (even when on the internet, "individuals maintain the expectation that entities will not be able to collect such

broad swaths of personal information absent consent[]"); *Byars v. Goodyear Tire & Rubber Co.*, 2023 WL 1788553, at *4 (C.D. Cal. Feb. 3, 2023), at *5 (in analogous wiretapping case, finding "website users had a reasonable expectation of privacy" in their online interactions and denying motion to dismiss). Defendants' categorical pronouncements are contrary to the law.

Plaintiffs have plausibly plead their expectation of privacy. The question of whether an intrusion transgresses that expectation of privacy is a fact question; what constitutes acceptable data collection on the Internet is not as simplistic or static as Defendants would have it be but is in fact evolving. *Alves*, 2023 WL 4456956, at *6-7 ("the question of whether an intrusion transgresses the privacy statute is a fact question.") Defendants' motion should therefore be denied.

C. Plaintiffs have alleged sufficiently offensive conduct on behalf of Defendants.

Defendants' protestations to the contrary, Plaintiffs adequately plead offensive conduct. MTD 28-30. Defendants' proposed standard that "shame or humiliation" ought to be required would render even video cameras in a bedroom benign if the person observed were clothed rather than naked. Clearly this is not the standard. The act of surreptitiously wiretapping someone—non-stop and in real time—in the privacy of their home or on their personal mobile device whenever that person visits a website comprises highly offensive conduct. Courts faced with similar online invasions of privacy routinely uphold intrusion into seclusion claims. *See, e.g.*, *Nickelodeon*, 827 F.3d at 292 (finding defendant's behavior to be highly offensive where online tracking was accomplished through "deceit and disregard"); *In re Google,* 806 F.3d at 151 (finding conduct "highly offensive" where defendant's alleged intrusions were surreptitious). The act of concealing surreptitiously wiretapping, combined with the unfiltered, non-stop recording in real-time every time someone visits Defendants' website is highly offensive conduct. The emphasis is on the conduct, not on the nature of information surreptitiously tracked. Plaintiffs sufficiently plead the

outrageous nature of the intrusion at issue here. ¶¶ 73, 87, 91, 146-51, 210, 278-83, 322-31, 385-94, 427-33. Moreover, "whether an intrusion is highly offensive is not typically a question that should be resolved at the pleading stage." *Hazel,* 2023 2023 WL 3933073, at *5.

IV. Plaintiffs State a Viable Computer Fraud and Abuse Act ("CFAA") Claim.

Defendants argue Plaintiffs' CFAA claim is unavailing because the statute is limited to "hacking," but nowhere does the term "hacking" appear in the statute. Rather, the CFAA imposes civil liability on a defendant who (1) knowingly or intentionally accesses a protected computer, which is used in interstate commerce; (2) without authorization, or in excess of authorization; and (3) causes at least $5,000 in damage over a one-year period. *Tracfone Wireless, Inc. v. Adams*, 98 F. Supp. 3d 1243, 1252 (S.D. Fla. 2015); *Stirling Int'l Realty, Inc. v. Tansey Soderstrom*, 2015 WL 2354803, at *1 (M.D. Fla. May 15, 2015).

First, Defendants claim they did not "access" Plaintiffs' computers or mobile devices. MTD 31. This ignores CFAA conspiracy liability. 18 U.S.C. § 1030(b); *Cloudpath Networks, Inc. v. SecureW2 B.V.*, 2016 WL 153127, at *18 (D. Colo. Jan. 13, 2016). Plaintiffs alleged detailed facts about how Defendants conspired with SRPs to allow them to access Plaintiffs' computers and place SRC without consent. ¶¶ 35, 45, 51, 137-157. SRPs would not have access without Defendants' aid. Defendants contracted with and gave SRPs the ability to spy on their customers' internet browsing and access their confidential communications. This satisfies the definition of conspiracy: an agreement with another to commit an unlawful act. *See Cisco Sys. v. STMicroelectronics*, 2015 WL 3488923, at *3 (N.D. Cal. June 2, 2015).

Next, Defendants urge the Court to adopt a narrow definition of the statute's term "damage," arguing only *physical* destruction, impairment or damage to a computer system should qualify. MTD 32. Neither the statutory text nor the case law supports such a standard. In *United*

States v. Soybel, 13 F.4th 584, 595 (7th Cir. 2021), the court held the "broad definition of 'damage' covers *any* impairment." In *Soybel*, defendant disputed that he caused "damage" when he injected code that changed plaintiff's password. The court reasoned that "'damage' means '*any* impairment to the integrity or availability of data, a program, a system or information'." *Id.* at 595 (emphasis in original). "To 'impair' is to damage or make worse . . . by diminishing in some material aspect." *Id.* The court reasoned that defendant's actions of injecting code "impair[ed] . . . the . . . availability of ... [the] system" for plaintiff's use. *Id.*; *see also In re Toys R Us, Inc., Priv. Litig.*, 2001 WL 34517252, at *11 (N.D. Cal. Oct. 9, 2001) (CFAA claim sufficiently pled where plaintiffs alleged that Coremetrics' cookie is a "specially formatted text file" which defendants caused to be implanted in plaintiffs' computers without authorization); *Bowen v. Porsche Cars, N.A., Inc.*, 561 F. Supp. 3d 1362 (N.D. Ga. 2021) (CFAA adequately pleaded where plaintiff alleged that Porsche, without authorization, sent software update to vehicles that caused the vehicles to continuously reboot and plaintiff pleaded sufficient damages).

Here, Plaintiffs plead facts that Defendants impaired the value (integrity) of their private information by allowing SRPs to insert code on Defendants' websites on Plaintiffs' computers. ¶¶ 45, 51, 137-157; *see supra* Part I.A. Plaintiffs also plead facts supporting a finding of aggregate damages sufficient to meet the $5,000 CFAA minimum. ¶¶ 189-190. At the motion to dismiss stage, Plaintiffs have sufficiently plead a violation of the CFAA.[17]

V. Plaintiffs Adequately Plead their Unfair Competition Claims

[17] The cases relied upon by Defendants are inapposite. For example, in *Pipeline Productions, Inc. v. S&A Pizza, Inc.*, 2021 WL 4811206 (W.D. Mo. Oct. 14, 2021), the court explained that an allegation of economic harm or financial injury "not relate[d] to either responding to the offense [the unauthorized access] or consequential damages due to interruption of service" are not sufficient to withstand a Rule 12(b)(6) motion." But here, Plaintiffs plead their economic harm was related to unauthorized access of SRPs enabled by Defendants.

A. Plaintiff Durham and Moore Adequately Plead their California UCL Claims

Plaintiffs adequately plead their UCL claim. Defendants first contend that Plaintiffs lack statutory standing on the grounds they did not lose money or property as a result of the alleged misconduct. But that is incorrect. Plaintiffs allege that Defendants' interception and use of their personal information diminished its value, which is a recognized form of economic injury under the UCL. See *Calhoun v. Google LLC*, 526 F. Supp. 3d 605, 636 (N.D. Cal. 2021) ("[T]he Ninth Circuit and a number of district courts, including this Court, have concluded that plaintiffs who suffered a loss of their personal information suffered economic injury and had standing."). This unauthorized interception and use of Plaintiffs' valuable data confers standing under the UCL.

Defendants challenge Plaintiffs' claim under the unlawful prong by asserting that since the underlying predicate claims fail, the UCL claim must also fail. However, as predicate claims should not be dismissed, the UCL claim survives. *See supra.* Defendants next challenge Plaintiffs' claim under the unfair prong, falsely asserting that Plaintiffs merely recite the "South Bay" test without any factual support. A fair reading of both Plaintiffs' UCL claim as well as the numerous factual allegations throughout the complaint and incorporated in the UCL count demonstrate that the test is met. The "South Bay" balancing test was enunciated in *South Bay Chevrolet v. General Motors Acceptance Corp*., 72 Cal. App. 4th 861, 864 (Cal. App. 1999). Under that case, a practice is "unfair" "when it offends an established public policy or when the practice is immoral, unethical, oppressive, unscrupulous or substantially injurious to consumers." *Id.* The court then balances "the harm to the consumer against the utility of the defendant's practice." *Lozano v. AT&T Wireless Servs., Inc*., 504 F.3d 718, 735-36 (9th Cir. 2007). Plaintiffs allege that Defendants' actions in wiretapping Plaintiffs' communications were immoral and substantially injurious. Plaintiffs further allege that Defendants' actions offend established public policy. Certainly, Defendants'

actions offend an established public policy of the State of California for consumers to have their privacy protected under the Article I of the California constitution. Plaintiffs further balance the interests comparing the utility of the Defendants' conduct against the gravity of harm. ¶ 240. In any event, a decision on this issue is premature because the "South Bay" balancing test is fact intensive and not conducive to resolution at a motion to dismiss. *S*ee *McKell v. Wash. Mut., Inc.*, 142 Cal. App. 4th 1457, 1473 (Cal. App. 2006).

B. Plaintiff Tucker Adequately Pleads her MMPA Claim

The MMPA strictly prohibits "[t]he act, use or employment ... of any deception, fraud, false pretense, false promise, misrepresentation, or unfair practice ... in connection with the sale ... of any merchandise." R.S.Mo. § 407.020 (2017). As a result, the MMPA is not limited to consumers who make purchases in the marketplace. The intent and scope of the MMPA, which is "paternalistic," has a "fundamental purpose is the 'protection of consumers;'" "to promote that purpose, the act prohibits false, fraudulent or deceptive merchandising practices." *Huch v. Charter Commc'ns, Inc*., 290 S.W.3d 721, 724-27 (Mo. 2009) (en banc) (citations omitted). Missouri courts consistently reject arguments that "would effectively strip consumers of the protections afforded to them under [it] and unfairly allow companies" to insulate themselves from liability. *Id*. at 726-27; *see id.* (refusing to dismiss MMPA claims due to MMPA's broad, paternalistic intent).

The terms of the MMPA, particularly the term "unfair practice," must be liberally construed to protect consumers. According to the Supreme Court of Missouri, "[t]he literal words ['unfair practice'] cover every practice imaginable and every unfairness to whatever degree." *Ports Petroleum Co. Inc. of Ohio v. Nixon*, 37 S.W.3d 237, 240 (Mo. 2001) (en banc). As a result, it is hard to imagine a broader concept." *Id*. at 241; *see also Conway v. CitiMortgage, Inc.*, 438 S.W.3d 410, 416 (Mo. 2014). Plaintiff Tucker's allegations thus sufficiently establish an "unfair practice"

under Missouri law. *See* ¶ 374 ("Defendants omitted and/or concealed that they directed [SRPs] to secretly monitor, collect, transmit, and disclose their website visitors' Website Communications to the [SRPs] using [SRC]."). The MMPA certainly covers, situations like these in which Plaintiff Tucker sought to buy products on Defendants' websites and were advertised to by Defendants on their websites. *See* ¶¶ 127-31, 375.

Defendants' case law does not counsel otherwise. In *Freeman Health System v. Wass*, an uninsured plaintiff failed to remit payment to the hospital and asserted an MMPA counterclaim in Freeman's action to collect, claiming the insurance company was overcharging for copays. 124 S.W.3d 504, 506-507 (Mo. App. 2004). There, the court held that plaintiff, having failed to pay the bill in question, had not "purchased" services as required to constitute injury under the MMPA. *Id.* Critically, the *Freeman* plaintiff did not allege any other injury, such as a hit to his credit report due to overinflated bills. And in *Raster v. Ameristar Casinos*, *Inc.*, 80 S.W.3d 120, 129–30 (Mo. App. 2009), the court *upheld* the Plaintiffs' MMPA claim under the "purchase" language.

Plaintiff Tucker also alleges an "ascertainable loss." Plaintiff's personal information was taken/damaged as a result of his visiting Defendants' website to purchase products online and was diminished in value. ¶¶ 364-381; *see supra* Part I.A. MMPA damages or the lack thereof are also not a basis for dismissal at this stage; the long-standing rule of law in Missouri is that damages is a factual issue to be determined by a jury. "A jury's primary function is fact-finding, including the determination of damages." *Richardson v. State Highway & Transp. Com'n*, 863 S.W.2d 876, 880 (Mo. 1993) (citing *Jaycox v. Brune*, 434 S.W.2d 539, 542-43 (Mo. 1968)). Dismissal at this early stage would deprive Plaintiffs of their right to a jury's damages determination.

VI. Plaintiffs Adequately Plead their Conversion and Larceny Claims

A. Plaintiffs Adequately Plead Trespass and Conversion to Chattels

"A trespass to chattel may be committed by intentionally intermeddling with a chattel in the possession of another[.]" *Foremost Ins. Co. v. Pub. Serv. Comm'n of Mo.*, 985 S.W.2d 793, 797 (Mo. App. 1998); *see also Creative Dimensions in Mgmt., Inc. v. Thomas Grp., Inc.*, 1999 WL 225887, at *3 (E.D. Pa. Apr. 16, 1999) (citing Restatement (Second) of Torts § 217 (trespass to chattels requires intentional dispossession or use or intermeddling with a chattel of another); § 222 (the actor is subject to liability for conversion where the dispossession "seriously interferes with the right of the other")).[18] Furthermore, Plaintiffs pleaded a conversion claim. *See First Nat'l Bank of Steeleville v. ERB Equip. Co.*, 972 S.W.2d 298, 300 (Mo. Ct. App. 1998); *QVC, Inc. v. Resultly, LLC*, 159 F. Supp. 3d 576, 600 (E.D. Pa. 2016) (the elements of trespass to chattels "are essentially the same" as conversion). Conversion is a tort against the right of possession. *Id.*[19]

Defendants argue that Plaintiffs' trespass to chattels claim fails because they do not plead a *physical* interference. MTD 38. But chattel is defined as "[m]ovable or transferable property; esp. personal property," and "[p]ersonal chattel is defined as a 'tangible good or an intangible right.'" *Weicht v. Suburban Newspapers of Greater St. Louis, Inc.*, 32 S.W.3d 592, 600 (Mo. App. 2000) (quoting Chattel, Black's Law Dictionary (7th ed. 1999)) (analyzing a claim of malicious trespass). Although not addressing a trespass to chattel claim, the Missouri Supreme Court stated

---

[18] "Under California common law, the tort of trespass to chattel encompasses unauthorized access to a computer system where (1) defendant intentionally and without authorization interfered with plaintiff's possessory interest in the computer system; and (2) defendant's unauthorized use proximately resulted in damage to plaintiff." *Craigslist Inc. v. 3Taps Inc.*, 942 F. Supp. 2d 962, 980 (N.D. Cal. 2013) (internal citation and quotations omitted).

[19] Trespass to a chattel and conversion of a chattel differ in that (1) conversion relates to personalty only, while trespass relates to both personalty and realty; (2) conversion is usually characterized by a wrongful exercise of dominion and ownership over personalty interfering with owner rights where the only wrong may be a refusal to surrender a possession which was originally rightful, but for which the right has terminated, while trespass always involves an unlawful taking. *Tubbs v. Delk*, 932 S.W.2d 454, 456 (Mo. Ct. App. 1996) (citing 87 C.J.S. Trespass § 3 (1954)).

"[p]ersonal property can be either tangible or intangible." *Norris v. Norris*, 731 S.W.2d 844, 845 (Mo. 1987) (*en banc*) (construing a will).[20]

As a result, Plaintiffs plausibly plead claims for trespass to chattel and conversion based on Defendants' actions to deprive Plaintiffs of their intangible personal property, specifically, their intangible data tied to something tangible – *i.e.*, their devices and Microsoft Azure and/or Google Servers.[21] ¶ 453. Plaintiffs allege that the "Session Replay Providers also accessed Plaintiffs' and the Class Members' data, systems, and networks without their permission, authorization, or consent." ¶ 183. Specifically, SRC "procured by Defendants surreptitiously and instantaneously intercepted, stored, and recorded everything Plaintiffs and Class Members did on Defendants' websites, *e.g.*, what they searched for, what they looked at, the information they inputted, and what they clicked on for the entire duration of their visit." ¶ 2; *see* ¶ 67. This constitutes an action by Defendants to intentionally, directly or through a third party, interfere or intermeddle with, and to take, use and transfer property from Plaintiffs and Class Members, and to exercise control or authority inconsistent with Plaintiffs' and Class Members' use and/or possession of the data contained on Plaintiffs' devices as described above. ¶ 463. And Defendants used Plaintiffs' and Class Members' devices by placing Session Replay Code directly on their devices for the purpose

---

[20] Missouri courts and others have determined that digital objects and accounts can constitute intangible personal property for purposes of a cause of action for conversion and/or trespass to chattels. *See Porters Bldg. Ctrs., Inc. v. Sprint Lumber*, 2017 WL 4413288, at *15 (W.D. Mo. Oct. 2, 2017) (e-mails are intangible personal property, and thus a chattel, because the email communication is connected to a tangible server, denying summary judgment); *Skapinetz v. CoesterVMS.com, Inc*., 2018 WL 805393 (D. Md. Feb. 9, 2018) ("[M]any courts have recognized claims for conversion or trespass to chattels involving digital 'property'."); *see also Grace v. Apple Inc.*, 2017 WL 3232464, at *11 (N.D. Cal. July 28, 2017) (citing *Kremen v. Cohen*, 337 F.3d 1024, 1030 (9th Cir. 2003)).

[21] Plaintiffs also adequately allege intent and that the actions were unauthorized in the sections regarding consent and intrusion upon seclusion above. *See supra* Part II.G & III.A; ¶¶ 446, 463.

of tracking Plaintiffs' interactions with the website that they would not have been able to track but for procurement and placement of SRC. ¶ 464. This disclosure and loss of privacy and confidentiality caused Plaintiff and the Missouri Class to experience mental anguish, emotional distress, worry, fear, and other harms. *Id.*

Finally, Plaintiffs adequately allege that Defendants' trespass and conversion diminished the value of Plaintiff's personal property. ¶ 379; *see supra* Part I.A. The aforementioned interference was the actual and proximate cause of injury to Plaintiffs because it exposed their private, personal and sensitive information and data to one or more third parties. ¶ 401.

B. Plaintiffs Sufficiently Plead their Statutory Larceny Claim

First, Defendants' illicit copying of Plaintiffs' personal data and information constitutes theft, even where the victim retains the original. "California courts have held that copying is theft because although the owner may retain possession of the original property, there has been nevertheless a deprivation of property when a copy is made." *Calhoun*, 526 F. Supp. 3d at 635 (internal quotation omitted). Countless other California courts have also held that unlawful copying of customer lists, files, telephone directories, trade secrets, and more, is larceny even where the victim retains the original. *E.g.*, *People v. Gopal*, 171 Cal. App. 3d 524, 541 (Cal. App. 1985); *People v. Parker*, 217 Cal. App. 2d 422, 427-8 (Cal. App. 1963); *Williams v. Superior Ct.*, 81 Cal. App. 3d 330, 341 (Cal. App. 1978). This is sufficient to assuage any concerns about the permanency of the theft, or that Plaintiffs fail to allege an injury.

Second, Plaintiffs plead their larceny count with sufficient particularity to survive Fed. R. Civ. P. 9(b). The California Penal Code states that persons who defraud other persons of personal property by false pretense are guilty of theft. Cal. Penal Code § 484(a). Cal. Penal Code § 496(c) provides a private right of action for "[a]ny person who has been injured" by the sale of stolen

property. Cal. Penal Code § 496(c). Thus, regardless of Plaintiffs' entitlement to a cause of action under § 484, due to the incorporation of theft by false pretense by § 496, Plaintiffs have alleged a claim for theft by false pretense.

Plaintiffs need not identify the exact type of theft Defendants committed. *People v. Ashley*, 42 Cal. 2d 246, 258 (Cal. 1954). The allegations underlying Plaintiffs' claim for violation of § 496(a) constitute larceny by trick, for which a lack of consent is not an element. *People v. Williams*, 57 Cal. 4th 776, 788 (Cal. 2013). Larceny by trick "involves fraudulently acquiring possession, but not title, of property." *People v. Gonzales*, 2 Cal.5th 858, 864 n.6 (Cal. 2017). "[T]he offense [of larceny] is committed by every person who (1) takes possession (2) of personal property (3) owned or possessed by another, (4) by means of trespass and (5) with intent to steal the property, and (6) carries the property away." *Harris v. Garcia*, 734 F. Supp. 2d 973, 999 (N.D. Cal. 2010). "The act of taking personal property from the possession of another is always a trespass [or nonconsensual] unless the owner consents to the taking freely and unconditionally" (theft by false pretenses), but "[w]hen the consent is procured by fraud it is invalid and the resulting offense is commonly called larceny by trick and device." *People v. Davis*, 19 Cal. 4th 301, 305 n.3 (Cal. 1998). The "intent requirement . . . is satisfied by the intent to deprive temporarily but for an unreasonable time so as to deprive the person of a major portion of its value or enjoyment." *People v. Avery*, 27 Cal. 4th 49, 58 (Cal. 2002). Here, Plaintiffs allege they were deprived both of their personal data and their devices when information was copied from them through the use of Session Replay Code. ¶¶ 446-47, 463-64.

CONCLUSION

For all of the reasons stated herein, Defendants' motion should be denied in its entirety.

Date: September 22, 2023

By: */s/ Nicholas A. Colella*

Nicholas A. Colella (PA Bar # 332699)
Gary F. Lynch (PA Bar # 56887)
Kelly K. Iverson (PA Bar # 307175)
Jamisen Etzel (PA Bar # 311514)
Elizabeth Pollock-Avery (PA Bar # 314841)
Patrick Donathen (PA Bar # 330416)
LYNCH CARPENTER, LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
Tel: (412) 322-9243
NickC@lcllp.com
Gary@lcllp.com
Kelly@lcllp.com
Jamisen@lcllp.com
Elizabeth@lcllp.com
Patrick@lcllp.com

Kate M. Baxter-Kauf
Karen Hanson Riebel
Maureen Kane Berg
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Avenue South, Suite 2200
Minneapolis, MN 55401
Tel: (612) 339-6900
kmbaxter-kauf@locklaw.com
khriebel@locklaw.com
mkberg@locklaw.com

Katrina Carroll
LYNCH CARPENTER, LLP
111 W. Washington St. Suite 1240
Chicago IL 60602
Tel: (312) 750-1265
katrina@lcllp.com

Joseph H. Kanee
MARCUS & ZELMAN LLC
701 Brickell Avenue, Suite 1550
Miami, FL 33131
Tel: (786) 369-1122
joseph@marcuszelman.com

Ari H. Marcus (PA Bar # 322283)
MARCUS & ZELMAN LLC
701 Cookman Avenue, Suite 300

Asbury Park, NJ 07712
Tel: (732) 695-3282
ari@marcuszelman.com
Plaintiffs' Co-Lead and Liaison Counsel

Carey Alexander
SCOTT & SCOTT, ATTORNEYS AT LAW, LLP
230 Park Avenue
Ste 17th Floor
New York, NY 10169
Tel: (212) 223-6444
calexander@scott-scott.com

MaryBeth V. Gibson
THE FINLEY FIRM, P.C.
3535 Piedmont Rd.
Building 14, Suite 230
Atlanta, GA 30305
Tel: (404) 978-6971
mgibson@thefinleyfirm.com

Steven M. Nathan
HAUSFELD LLP
33 Whitehall Street Fourteenth Floor
New York, NY 10004
Tel: (646) 357-1100
snathan@hausfeld.com

James J. Pizzirusso (Md. Bar No. 20817)
HAUSFELD LLP
888 16th Street N.W. Suite 300 Washington, D.C. 20006
(202) 540-7200
jpizzirusso@hausfeld.com
Plaintiffs' Steering Committee